

inhibiting the end station from receiving traffic addressed to the multicast group if the multicast group fails to conform with the multicast group authorization.

Claim 15 (Original): The method of claim 14, further comprising receiving the multicast group authorization in response to verification of a credential submitted by the end station.

Claim 16 (Original): The method of claim 15, wherein the credential is a user credential.

Claim 17 (Original): The method of claim 14, wherein the association of the multicast group authorization with the end station is inferred from an association of the multicast group authorization with a port through which the end station is known to access the network.

Claim 18 (Original): The method of claim 14, wherein the receiving, determining and inhibiting steps are performed on a LAN switch interposed between the end station and a router.

Claim 19 (Original): The method of claim 14, wherein the multicast group corresponds to an IP Multicast data stream.

Claims 20-23 (Cancelled).

Claim 24 (Original): A LAN switch, comprising:

a port for receiving a join message from a router regarding an end station;

and

a switch manager for receiving the join message from the port, for determining whether a multicast group in the join message conforms with a multicast group authorization associated with the end station and for inhibiting the end station from receiving traffic addressed to the multicast group if the multicast group fails to conform with the multicast group authorization.

Claim 25 (Original): The switch of claim 24, wherein the switch manager receives the multicast group authorization from an authentication server in response to verification by the authentication server of a credential submitted by the end station.

Claim 26 (Original): The switch of claim 24, wherein the credential is a user credential.

Claim 27 (Original): The switch of claim 24, wherein the association of the multicast group authorization with the end station is inferred from an association of the multicast group authorization with a port through which the end station is known to access traffic from the router.

Claim 28 (New): In a data communication network, a method performed on a second node communicating with a first node over a LAN link for controlling access of the first node to a multicast group, comprising the steps of:

- receiving from the first node authentication information;
- transmitting to an authentication server the authentication information;
- receiving from the authentication server in response to the authentication information multicast group authorization information; and
- storing in a database on the second node information based on the multicast group authorization information; then,
- receiving from the first node a management packet having multicast group membership information;
- comparing for conformance the multicast group membership information with the information stored in the database; and
- authorizing transmission to the first node of data packets addressed to a multicast group in response to a finding of conformance.

Claim 29 (New): The method of claim 28 wherein the authentication information comprises a user credential.

Claim 30 (New): The method of claim 28 wherein the multicast group authorization information is indicative of one or more multicast groups.

Claim 31 (New): The method of claim 28 further comprising the step of receiving from the authentication server in association with the multicast group authorization information an identifier of a port on the second node over which the first node and the second node communicate.

Claim 32 (New): The method of claim 31 wherein the port is a physical port.

Claim 33 (New): The method of claim 31 wherein the port is a logical port.

Claim 34 (New): The method of claim 28 wherein the multicast group authorization information is a RADIUS attribute within an EAP success packet.

Claim 35 (New): The method of claim 28 wherein the storing step further comprises adding an entry to the database associating a port on the second node over which the first node and the second node communicate with information indicative of one or more multicast groups.

Claim 36 (New): The method of claim 28 wherein the management packet comprises an IGMP membership report.

Claim 37 (New): The method of claim 28 wherein the data packets are IP Multicast data packets.

Claim 38 (New): The method of claim 28 wherein the second node supports a plurality of IP Multicast extension protocols enhanced with respective authorization checks.

Claim 39 (New): The method of claim 38 wherein the IP Multicast extension protocols comprise IGMP Snooping and CGMP.

Claim 40 (New): In a data communication network, a method performed on a second node communicating with a first node over a LAN link for controlling access of the first node to a multicast group, comprising the steps of:

- receiving from the first node authentication information;
- transmitting to an authentication server the authentication information;
- receiving from the authentication server in response to the authentication information multicast group authorization information; and
- storing in a database on the second node information based on the multicast group authorization information; then,
- receiving from a router a management packet having multicast group membership information regarding the first node;

comparing for conformance the multicast group membership information with the information stored in the database; and

authorizing transmission to the first node of data packets addressed to a multicast group in response to a finding of conformance.

Claim 41 (New): The method of claim 40 wherein the multicast group authorization information is a RADIUS attribute within an EAP success packet.

Claim 42 (New): The method of claim 40 wherein the storing step further comprises adding an entry to the database associating a port on the second node over which the first node and the second node communicate with information indicative of one or more multicast groups.

Claim 43 (New): The method of claim 40 wherein the management packet comprises a CGMP join message.

Claim 44 (New): The method of claim 40 wherein the second node supports a plurality of IP Multicast extension protocols enhanced with respective authorization checks.